



GEORGE MASON UNIVERSITY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2017

Auditor of Public Accounts
Martha S. Mavredes, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

We have audited the basic financial statements of George Mason University (George Mason) as of and for the year ended June 30, 2017, and issued our report thereon, dated April 5, 2018. Our report, included in George Mason's Annual Report, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at George Mason's website at www.gmu.edu.

Our audit of George Mason for the year ended June 30, 2017, found:

- the financial statements are presented fairly, in all material respects;
- two internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- two instances of noncompliance or other matters required to be reported under Government Auditing Standards.

–TABLE OF CONTENTS–

	<u>Pages</u>
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-2
INDEPENDENT AUDITOR’S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	3-5
UNIVERSITY RESPONSE	6-8
UNIVERSITY OFFICIALS	9

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Information Security Policies and Procedures

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

George Mason University (University) bases its information security policies and procedures on the ISO/IEC 27002 Security Standard (Security Standard). However, the University does not manage the information security program based on the current version of the Security Standard. The University uses ISO/IEC 27002:2005, which is no longer valid. ISO/IEC 27002:2013 superseded ISO/IEC 27002:2005 in September 2013. The University is currently reviewing and evaluating its information security policies and procedures to determine if the ISO/IEC 27002 Security Standard is the best fit to support and maintain the University's information technology (IT) environment and network.

The current version of the Security Standard, ISO/IEC 27002:2013, Section 5, requires the University to define, approve, communicate to employees, and periodically review a set of policies for information security, in addition to defining and publishing procedures that mandate effective implementation of information security controls. Without using a current Security Standard version, the University policies and procedures will not contain processes to support control requirements that align with current technologies. The University cannot effectively communicate security requirements to protect and mitigate risks to data without current and approved information security policies. Additionally, the University may inconsistently address security needs across the IT environment, potentially resulting in unauthorized access to data or the inability to recover from system outages promptly, among other risks.

The University does not have a process to periodically review and revise its information security policies and procedures, which led to the policies and procedures being out-of-date. In addition, the University does not have an individual responsible for maintaining current IT policies and procedures.

The University should revise and update all information security policies and procedures to align with the requirements in the current ISO 27002 Security Standard version. Once the University selects the most appropriate security standard to support their information security program, they should assign an individual that is responsible for maintaining the University's IT security policies and procedures to ensure they remain current. Having policies and procedures that align with a current Security Standard will help to protect the confidentiality, integrity, and availability of the University mission critical and sensitive data.

Improve Firewall Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

Repeat: No

The University does not properly secure the firewall that safeguards its secure internal network in accordance with its information security standard, ISO/IEC 27002 (Security Standard).

We communicated five separate control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should develop a plan to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the University secures its network to protect its systems and data.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

April 5, 2018

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Robert D. Orrrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

Board of Visitors
George Mason University

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and aggregate discretely presented component units of **George Mason University** as of and for the year ended June 30, 2017, and the related notes to the financial statements, which collectively comprise George Mason's basic financial statements and have issued our report thereon dated April 5, 2018. Our report includes a reference to other auditors. We did not consider internal controls over financial reporting or test compliance with certain provisions of laws, regulations, contracts, and grant agreements for the financial statements of the component units of George Mason, which were audited by other auditors in accordance with auditing standards generally accepted in the United States of America, but not in accordance with Government Auditing Standards.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered George Mason's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of George Mason's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of George Mason's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Improve Information Security Policies and Procedures" and "Improve Firewall Security," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether George Mason's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings entitled "Improve Information Security Policies and Procedures" and "Improve Firewall Security."

George Mason's Response to Findings

We discussed this report with management at an exit conference held on April 2, 2018. George Mason's response to the findings identified in our audit is described in the accompanying section titled "University Response." George Mason's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Status of Prior Findings

George Mason has taken adequate corrective action with respect to audit findings reported in the prior year.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

ZLB/clj



Jennifer Wagner Davis
Senior Vice President for Administration and Finance
4400 University Drive, MS 3B2, Fairfax, Virginia 22030
Phone: 703-993-8750; Fax: 703-993-8772

April 6, 2018

Martha S. Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2017 audit by the Auditor of Public Accounts (APA) and discussed during the exit conference.

George Mason University acknowledges and concurs with the audit findings. The following contains APA's finding, Improve Database Security, and management's response to the concerns and issues raised.

Improve Information Security Policies and Procedures

George Mason University (University) bases its information security policies and procedures on the ISO/IEC 27002 Security Standard (Security Standard). However, the University does not manage the information security program based on the current issue of the Security Standard. The University uses ISO/IEC 27002:2005, which is no longer valid. ISO/IEC 27002:2013 superseded ISO/IEC 27002:2005 in September 2013. The University is currently reviewing and evaluating its information security policies and procedures to determine if the ISO/IEC 27002 Security Standard is the best fit to support and maintain the University's information technology (IT) environment and network.

The current issue of the Security Standard, ISO/IEC 27002:2013, Section 5, requires the University to define, approve, communicate to employees, and periodically review a set of policies for information security, in addition to defining and publishing procedures that mandate effective implementation of information security controls. Without using a current Security Standard version, the University policies and procedures will not contain processes to support control requirements that align with current technologies. The University cannot effectively communicate security requirements to protect and mitigate risks to data without current and approved information security policies. Additionally, the University may inconsistently address security needs across the IT environment, potentially resulting in unauthorized access to data or the inability to recover from system outages promptly, among other risks.

The University does not have a process to periodically review and revise its information security policies and procedures, which led to the policies and procedures being out-of-date. In addition, the University does not have an individual responsible for maintaining current IT policies and procedures.

The University should revise and update all information security policies and procedures to align with the requirements in the current ISO 27002 Security Standard version. Once the University selects the most appropriate security standard to support their information security program, they should assign an individual that is responsible for maintaining the University's IT security policies and procedures to ensure they remain current. Having policies and procedures that align with a current Security Standard will help to protect the confidentiality, integrity, and availability of the University mission critical and sensitive data.

Improve Firewall Security

The University does not properly secure the firewall that safeguards its secure internal network in accordance with its information security standard, ISO/IEC 27002 (Security Standard).

We communicated five separate control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires the documentation and implementation of certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of the University's information systems and data.

The University should develop a plan to implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner. Doing this will help to ensure the University secures its network to protect its systems and data.

Management's Response

Improve Information Security Policies and Procedures

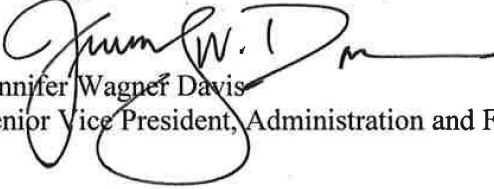
The University acknowledges that the current IT Security Standard based on ISO/IEC 27002:2005 is outdated. Due to emerging federal requirements pertaining to the treatment of Controlled Unclassified Information (CUI), the University's Information Technology Security Office has decided to base the new Security Standard on NIST SP 800-53 rather than the 2013 revision of the ISO standard. The NIST standards more directly support the CUI requirements, while still providing a comprehensive framework for protecting the broader University environment.

The University will update current policies and procedures, and create new ones as required, to align with the new IT Security Standard by 6/30/2019. The University's Information Technology Services division will formalize the responsibility for maintaining policies and procedures by 6/30/2018.

Improve Firewall Security

The University concurs with the recommended additional controls described in the FOIA Exempt management letter. Corrective actions for the cited control deficiencies will be addressed in a timely manner as detailed in the corrective action plan.

Sincerely,

A handwritten signature in black ink, appearing to read "Jennifer W. Davis", with a long horizontal flourish extending to the right.

Jennifer Wagner Davis
Senior Vice President, Administration and Finance

GEORGE MASON UNIVERSITY

As of June 30, 2017

BOARD OF VISITORS

Thomas M. Davis, Rector

Jon Peterson, Vice Rector

Kelly McNamara Corley, Secretary

Mahfuz Ahmed	John Jacquemin
Karen Alcalde	Wendy Marquez
Stephen M. Cumbie	David Peterson
Claire Dwoskin	Shawn Purvis
Anne Gruner	Tracy Schar
James Hazel	Robert Witeck
Lisa Zuccari	

Keith D. Renshaw, Faculty Representative

Nathan Pittman, Student Representative

Christian Suero, Student Representative

UNIVERSITY OFFICIALS

Àngel Cabrera, President

Jennifer Davis, Senior Vice President for Administration and Finance

Lisa Kemp, Associate Vice President and Controller